Federal Ministry
for Economic Cooperation
and Development

IT and cybersecurity in the financial sector

Growing cybercrime calls for innovative solutions

Financial institutions in emerging economies and developing countries are increasingly the target of cyberattacks

Digital theft through ever more complex cyberattacks are a reality in the digital financial sector worldwide. Small and medium-sized financial institutions in emerging economies and developing countries that fail to invest enough in the necessary security of their systems are at particular risk.

Cyberattacks on Bangladesh Bank

In 2016, hackers tried to steal USD 951 million from the Bangladesh central bank. In the end, they were able to obtain USD 81 million by infiltrating the internal IT system and manipulating transfers.

With the rapidly growing use of digital financial products and virtual interaction, cyber threats to providers outside their own network are also on the rise as a result of insecure mobile devices used by customers. This is problematic in developing countries in particular, where people are often more likely to have a mobile wallet than a traditional bank account. A study by the University of Florida shows that most mobile wallet applications have data- and system-security loopholes: only one of the 46 applications tested was considered secure.

All this poses a number of challenges for regulatory and supervisory authorities in partner countries of German development cooperation. In addition to financial institutions' weak cyber defence systems and limited personnel and financial capacity to set up these systems, challenges include obstacles to criminal prosecution. Complex issues also arise in terms of jurisdiction, powers, cross-border cooperation and the consistency of cybercrime laws across different countries.

The international community is responding – but is still hesitant

According to the International Organisation of Securities Commissions (IOSCO), cybersecurity threats threaten the integrity, efficiency and robustness of global financial markets. In 2016, the G7 countries addressed the widespread effects of increasingly frequent and complex cyberattacks on financial institutions and founded the Cyber Expert Group (CEG), which identifies cyber risks for the financial sector and develops approaches to action. In 2017, the G20 finance ministers and the heads of central banks agreed that cyberattacks pose a constant threat to the entire financial system. They said that ongoing measures were needed to ensure the cyber resilience and cyber security of the financial sector. This aspect is also part of the digitalisation strategy of the German Federal Ministry for Economic Cooperation and Development (in German) which provides development policy support for IT solutions and ensures that these are appropriately secure and that staff are trained to use them securely.

Engaging German development cooperation

German development cooperation works with central banks and supervisory authorities, banking and insurance associations and partners in the IT sector to support the development of capacity in the areas of IT and cyber resilience. To do so, it draws on the experience of the German regulatory and supervisory legislative framework on cyber security in the financial sector and passes on the necessary knowledge. This includes, for example, dialogue between the public and private sector and private sector measures, particularly those implemented by financial institutions, to improve their own cyber resilience.

Data and IT security for a health risk management app in India and Pakistan

In a strategic alliance with Allianz SE, the insurtech company BIMA and start-up Medicount, a health risk management app was developed that collects and uses a large amount of sensitive data. Simulated hack attacks on the app help to identify and fix security gaps. To guarantee the protection of personal data, standards based on the EU General Data Protection Regulation (GDPR), including data protection notices for customers, among other things, are integrated.

German development cooperation also focuses on compliance with international cybersecurity standards. A checklist for cybersecurity developed specifically for financial cooperation (FC) projects is also used in this context. This allows for an initial risk assessment of FC project partners in information security, data protection and cybersecurity, which forms the basis for deciding whether a more detailed cybersecurity analysis is needed.

Recommendations for stakeholders in international development cooperation

- Raising awareness among financial institutions, insurance companies, managers and supervisory authorities of the need for cyber security strategies
- Supporting coordination between financial sector authorities and financial institutions, including insurance companies and other institutions managing cyber risks and cyber security
- Designing and promoting initial and continuing training programmes for technical specialists and qualified analysts and developing cyber resilience training programmes for regulatory authorities and financial institutions
- Supporting supervisory authorities in advising financial institutions and consumers
- Supporting creation of networks and capacity in order to make the IT systems of financial institutions more secure, e.g. by setting up a technical firewall
- Promoting the education and awareness of internet users in partner countries in relation to cyber crime

Published by
Federal Ministry for Economic Cooperation and Development (BMZ)
Division 110

As at:
11/2020September 2020

Contact
RL110@bmz.bund.de
www.bmz.de

Address of BMZ offices
BMZ Berlin
Stresemannstraße 94
10963 Berlin, Germany
T +49 (0)30 18 535-0

BMZ Bonn
Dahlmannstraße 4
53113 Bonn, Germany
T +49 (0)228 99 535-0

Edited by
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Economic and Social Development, Digitalisation Division
Financial Systems Development Sector Project

Contact: sv.fse@giz.de
www.giz.de